Legal Aspects of the Security Concerns Surrounding Radio Frequency Identification (RFID) Technology

Abu Hena Mostofa Kamal*

Abstract

Radio Frequency Identification (RFID) is regarded as technological perfection. RFID is a technology used for tracking items and auto identification. This automated data-capture technology allows the user to remotely identify a person, place, or thing, and instantly associate it with stored data. It offers wireless communication between RFID chips and readers. RFID is increasingly used in the developed countries within electronic identification cards, passports and vehicle identification. Regrettably, this technology can be used for gathering information about an individual that traditionally would require a warrant based on probable cause. These new and possibly nefarious uses of RFID raised serious privacy issues. This paper explains the operation of RFID technology, its potential benefits and applications, the threat it poses to the citizens specially consumers and its likely impact on Bangladeshi legal regime. This article mainly looks at privacy issues relating to the use of RFID, and suggests the desired parameters to these systems which are consistent with present privacy laws of Bangladesh, as well as comments on whether the present privacy laws adequately protect consumers from retail surveillance.

Keywords: Radio frequency identification; Privacy; Computer security; Data protection; Data storage; Personal data; Radio frequency identification

"We must protect our citizens' privacy -- the bulwark of personal liberty, the safeguard of individual creativity." ~*Bill Clinton*

Introduction

As the proliferation of Radio Frequency Identification (RFID) technology becomes more and more prevalent, concern about 'personal privacy and security' becomes a more pressing topic. In our society, tailored and individualised services transmitted through RFID, appears to gain unprecedented popularity. In recent years RFID technology has spawned many privacy and security issues as RFID unlike other technologies support a greater capturing of customer and user information and allow services to be tailored to the owner's needs and desires which can be subject to misuse.[i] Confidential information in relation to individuals (members, customers, patients or citizens) may allow unscrupulous entrepreneurs or commercial and public sector organisations to identify and address a large number of people on an 'individualised basis' not only within their territorial periphery but even internationally. [ii] Like mobile tracking facilities, RFID can be used for track and trace other individuals and these tracking facilities may trigger various intrusions to individual's privacy if not regulated by stringent rules. Location-based RFID

*Assistant Professor, Department of Law, ASA University Bangladesh

offers almost limitless surveillance capacities which may be used for "unlawful purposes undermining the interest of societal values behind the very notion of privacy as a legal entitlement, values such as autonomy, control, transparency and digital diversity."[iii] As we know, the laws relating to privacy of individuals are built on deep assumptions about information asymmetries and information control. In recent time, personal information becomes more widely gathered and harder to restrict due to the emergence of new technologies like RFID. As a result assumptions relating to privacy are undermined to a great extent, causing the judiciary to struggle for interpreting rules to accommodate the changed circumstances.

But what, really, is "RFID"?

As said before, RFID technology offers wireless communication between RFID tags and readers with non-line-of-sight readability. RFID stores and retrieves information remotely. These fundamental properties eliminate manual data entry and introduce the potential for automated processes to increase productivity. RFID tags consist of a microchip connected to an antenna, which is constructed of a small coil of wires. The assembly is usually covered with a protective layer, which is determined by the type of application. Components of passive RFID system are as follows:

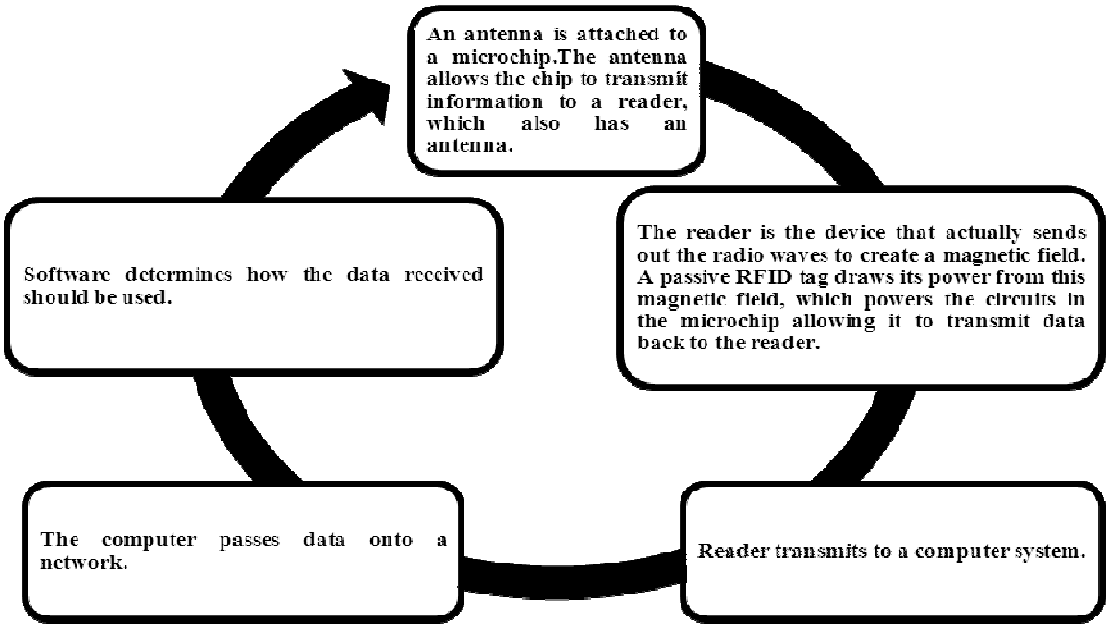


Figure 01-A: Components of passive RFID system.

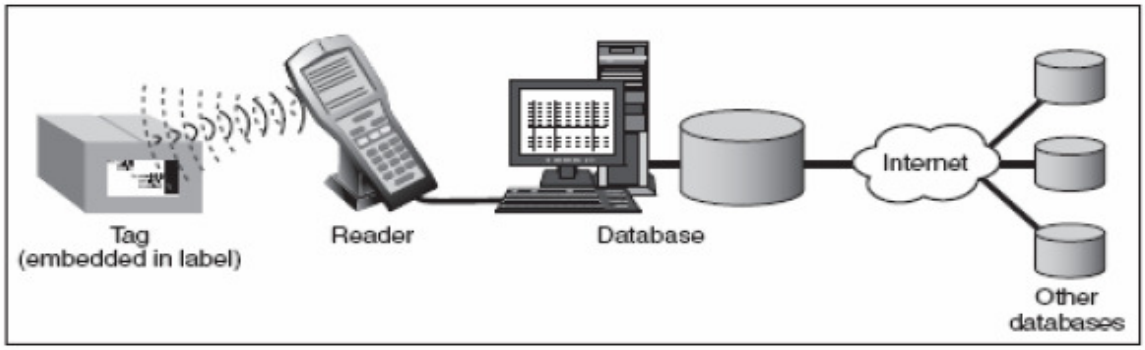


Figure 1-B: Main components of the RFID system. Source: GAO[iv]

RFID has been used for over 30 years in various countries and were immensely used in many car keys and bank cards, passports, library cards, student identification cards and, national identity cards. Customised RFID tags can hold up to 32 mega-bytes[v] of information which makes them counterfeit proof. The data on existing RFID tags can be changed or updated. Recently RFID is used in products instead of bar codes. RFID tags and readers are cheap and economically feasible. The economic viability and its storage and interactive communication capacity makes it much more useful than bar codes. In addition, an RFID tag provides a unique identifier for each product equipped with it. The US State Department has recently initiated the process to embed RFID chips in passports.[vi] Major pharmaceutical companies are putting RFID chips in prescription drug bottles to combat counterfeiting and fraud.[vii] RFID tagging isn't limited to inanimate objects. Many pets already have tags embedded under their skin to help retrieve them if they are lost or stolen. In some countries, people have volunteered to have chips embedded under their skin to protect against kidnapping[viii] or to provide easy access to exclusive dance clubs.[ix] Schools in Asia are putting RFID tags in student's clothes or backpacks as a security measure. One variation of RFID chip called 'the VeriChip'[x] is designed to go under the skin, where it can be read from four feet away. These chips are used for keeping track of children, Alzheimer's patients in danger of wandering, and anyone else with a medical disability. In 1994, in conjunction with Operation Sea Signal, the U.S. government used RFID-tagged bracelets to track fifty thousand Haitian and Cuban refugees who were fleeing their native countries.[xi] In the past few years, human RFID trials were successfully conducted in U.S. For example, in 2004, the Robert Woods Johnson Foundation funded a three-month trial using RFID tags on indigent patients at The Elvis Presley Memorial Trauma Center. Each patient entering the emergency room was tagged with an RFID anklet so that he could be tracked by one of the twenty-five readers installed throughout the hospital.[xii] In countries such as Korea, China and Thailand, RFID is being used in contact-less smart cards for the purposes of travel, road tolls and national identification. In China, where ID cards are compulsory, the National People's Congress passed the National Citizens ID Law on 28 June 2003, which authorised the introduction of RFID-embedded ID cards to replace old-style plastic ones. The cards will include information such as name, age, gender, date of birth, address, national ID number, photo etc. The European Central Bank is seriously examining the idea of

embedding RFID in Euro notes. This would have the advantage of allowing banks to count large amounts of money in seconds, and would also help stem the tide of money laundering and counterfeiting. But RFID is to be allowed to be embedded in money, one of the last genuinely anonymous ways of living people's lives would cease to exist in an instant. Such a move would make it technologically possible for banks to know exactly how much money a person is carrying and would allow governments to track the passage of cash from person to person. Criminals with transceivers would be able to spot the best targets for their crimes, by being able to divine exactly how much money a person was carrying before they relieved him of it.

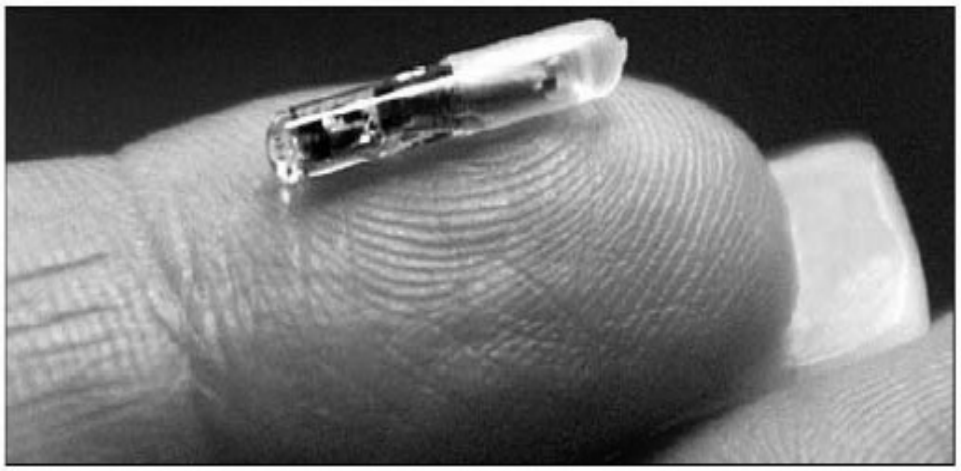


Figure 2: Human implantable RFID Chip -the 'VeriChip'. Source: RFID Chip[xiii]

How the RFID system entails the processing of personal data?

RFID technology is based on the use of an electronic chip linked to a miniature antenna. This technology generally appears in a form about the size of a grain of rice or a tag. There are three classifications of RFID tags: (1) passive (2) Semi-passive and (3) active. Passive tags depend on a power source provided by the RFID reader's energy field and may have read-write or read-only capabilities. Semi-passive RFID tags are very similar to passive tags except for the addition of a small battery. Semi-passive tag relies on the battery built into the tag to achieve a better performance within the operating range. This battery allows the tag IC to be constantly powered, which removes the need for the antenna to be designed to collect power from the incoming signal. Antennas can therefore be optimized for the backscattering signal. The active tags have an internal power source and are rewritable. In this category, the battery powers the internal circuitry during the communication; however, it is not used to generate radio wave.[xiv] Semi-passive tag is mostly fragile and expensive in the market.

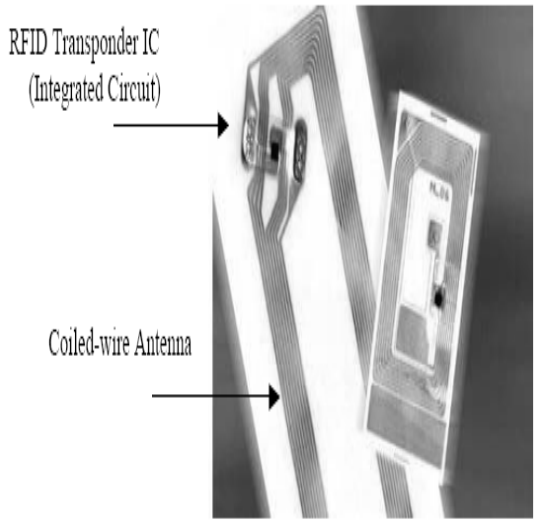


Figure 3: Antina sealed within RFID chip

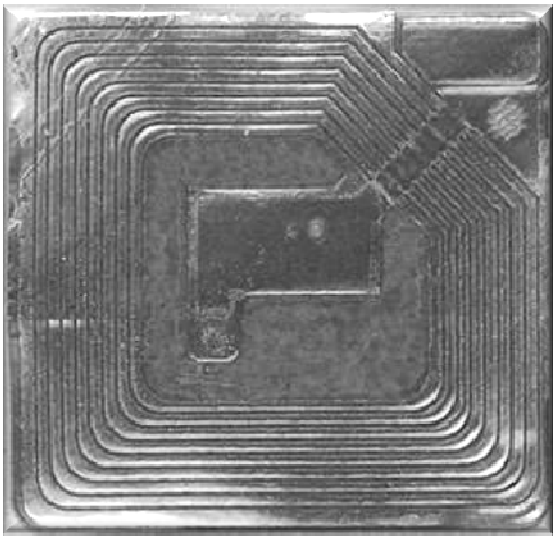


Figure 4: Insde the RFID

In most cases, RFID technology operates passively, without its own energy, awaiting activation by radio frequencies transmitted through transmitter-receivers (RFID readers). It uses the energy from the radio signal which it receives and reflects and responds to it. This passive RFID technology has a maximum range of about ten meters, while active RFID technology, which has an internal battery, has a greater range depending on the reader used. Passive tags generally have shorter read ranges but have a life that usually outlasts the object that it is identifying. Active tags have longer reading ranges, high memory, and better noise protection. However, these tags are larger and heavier, more expensive, and have a shorter life (3 – 10 years) than passive tags. Read-only tags are used for simple identification purposes because they can only store a limited amount of information that cannot be altered.

Presently, RFID tags are being produced with the design weight of 50 grams, a life cycle of being written to 100,000 times, data retention greater than 10 years without power, and the durability to withstand being dropped to concrete from a height of 1 meter a multiple number of times. Just as with other technologies, there are vulnerabilities with RFID technology, too. There are three major vulnerabilities with RFID technology. These are Viruses (and other types of attacks), Hacking (product and identity theft), and Tracking Misuse. Tracking Misuse is profoundly related to dissemination of private information without consent. Another example of misuse of RFID technology is the intellectual property infringement of the use of RFID enabled spare parts. The RFID enabled good, such as a car, computer or printer, could be programmed only to accept RFID enabled spare parts approved by the manufacturer. It is increasingly common for spare parts to be interrogated by the main product, in order to verify the legitimacy of the spare part. Such use of RFID technology would prevent third party manufacturers of compatible spare parts from competing with the manufacturers' own spare parts, which would ordinarily be more

expensive than the generic spare parts available from the third party manufacturers. Even more specifically, the RFID tag on the spare part could require that the customer only use the genuine spare parts where they are sourced directly from the manufacturer or from a select number of approved suppliers within Europe, such that the customer was precluded from taking advantage of price differentials pertaining in other European Member States, online via the internet or through parallel importers, in respect of the genuine manufacturers' spare parts. In this scenario, the customer will be forced to pay more for the spare parts since competition has been restricted on that market. Where the customer or third party supplier attempts to interfere with the RFID tag in order to circumvent the technological protection measures imbedded in the tag, such activities could be deemed a criminal offence.

Privacy Concerns and RFID

"Until they become conscious they will never rebel, and until after they have rebelled they cannot become conscious."- George Orwell, 1984

Though RFID is evolving as a major technology-enabler with numerous promising real-life business applications, it is not a novel technology as its applications can be traced back to World War II, when it was used by the British to recognise a fighter plane as a friend or an enemy. RFID is a powerful tracking technology that raises unprecedented privacy concerns. The regulatory and commercial developments in different legal regimes lead to different principles and approaches. Appropriately, these regimes are undertaking a multi-layered effort to ensure that RFID remains relevant, yet there should be certain pre-emptive measures for protecting privacy. Civil liberty Organisations have also raised their eyebrows questioning the legitimacy of RFID tracking technology. The technology reveals worried danger within the privacy sphere that needs to be defused. Though there are many advantages of RFID tags such as the ability to track items no matter where they go, the dark side of this technology is that it gives covert and unrestricted access to strangers raising legal, ethical and moral issues. When RFID chips are embedded in the ID cards or items in possession, effectively broadcasts its presence to anyone within range; hence, creating privacy issues. The main concern of RFID in object tracking is that the customers do not want themselves or their purchased products to be tracked once they own the products as it poses tremendous problems to the consumer's privacy. Further, RFID tags can be hidden inside objects without customer knowledge.[xv] This would make it possible for individuals to read the RFID tags for the lifetime of the product, without the consumer ever having knowledge of the tag's existence. Furthermore, many civil liberty groups are uncomfortable with this development by anticipating the creation of massive databases containing unique RFID tag data that can link tags and people, and then be used for unfair marketing.[xvi] Civil liberty groups, further fear that the unique identifying data stored in an RFID could be used for tracking and profiling individuals and for monitoring individuals. Consumer watchdogs are not the only ones voicing concerns. IT companies such as the cryptography producer RSA, have already shown evidence of just how vulnerable this technology is.[xvii] One of RSA's big worries lies in the ease with which the personal data contained in RFID tags can be acquired. Researchers from RSA Laboratories and Johns Hopkins University recently scanned the information on RFID chips in car keys and on Exxon Mobil Speed-Pass tags. They were able to collect enough information to crack the encryption codes on the tags. The researchers discovered the security flaws while studying the

Texas Instruments Registration and Identification System, according to news reports. The low-power radio-frequency security system they cracked is used worldwide. The Texas Instruments system is only one of a number of RFID systems on the market. Those with criminal intentions with the same knowledge of how to breach RFID tag security layers could steal the cars or buy free gas. RSA sees examples such as this as a sign that the backers of the RFID industry are being short-sighted by trying to roll out more uses for RFID devices before their security and privacy issues are addressed. A similar type of incident was happed in August 2006. [xviii] Nike, in conjunction with Apple, launched a new product geared towards runners: the Nike+ iPod Sport Kit[xix]. The $29 kit includes a nickel sized sensor that may be placed in a Nike running shoe, which communicates with a receiver that attaches to an iPod nano5 using RFID. When the runner moves, the sensor in the shoe signals the receiver in the iPod, which allows the runner to monitor distance travelled, calories burned and speed achieved.[xx] Scott Saponas, an avid runner and doctoral student at the University of Washington, was eager to purchase the Sport Kit. He soon realized, however, it could be used for non-athletic endeavours—like surreptitiously tracking the movement of others. With the aid of two other graduate students and a computer science professor, Saponas created several inexpensive RFID readers to detect the Nike sensors. From a remote location, they were able to detect anyone with a sensor who passed. Therefore we may under the above circumstances conclude that there exist privacy concerns within the RFID technology.

In the current era, safeguarding individual privacy and autonomy is a major concern. Any breach of an individual's privacy is a major ethical as well as legal issue. Such violation can be effectively dealt either by voluntary compliance to industry standards or mandatory regulation by the government. Regrettably, individuals have no control over RFID technology, particularly regarding the following points:

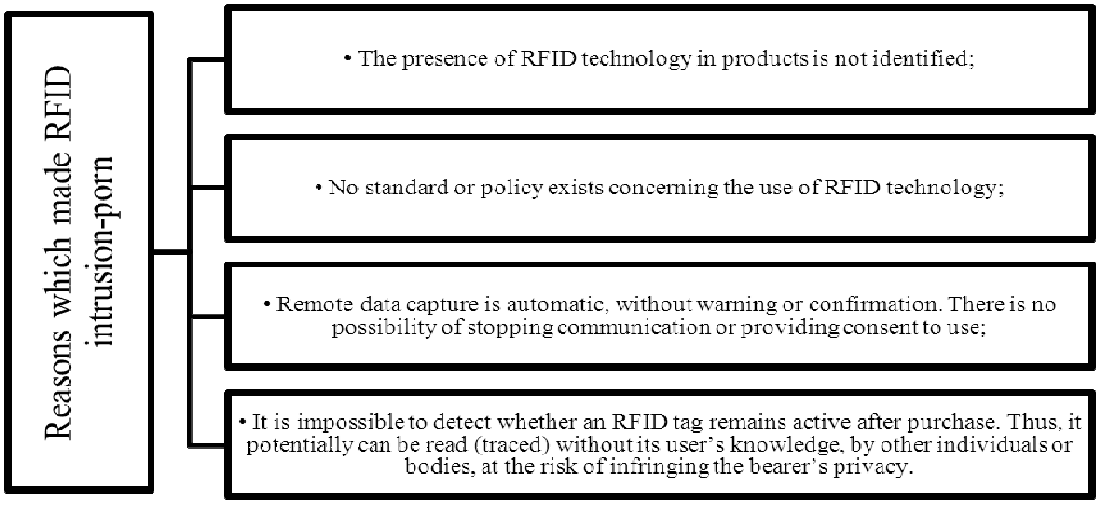
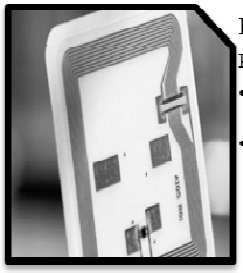


Figure 05: Reasons which made RFID intrusion-porn

As said earlier, any data contained in a RDFI chip can give rise to numerous intrusions for privacy. For example, a store can use an RFID tag with a unique number (EPC code) for a product and link this number to the buyer's name when payment is made by credit card. This information can be stored to establish consumer habits and brand preferences. This use of RFID chips is comparable to the use of cookies when surfing the Internet and thus could have similar impacts. Furthermore, most RFID tags can be easily counterfeited. It is easy to scan the bar code and lift the data from them. The technology is therefore likely to enable the creation of new crimes by thieves, blackmailers and stalkers. There are also other serious privacy concerns, as voiced by NGO's including the American Civil Liberties Union, the Electronic Frontier Foundation, The World Privacy Forum and a dozen other organisations.[xxi] These organisations ask for a voluntary moratorium on RFID technology in consumer goods, because the use of RFID could in their eyes enable an omnipresent police surveillance state, and it could make identity theft even easier than it has already become. It is pertinent to note that Benetton scrapped plans to embed RFID chips in its clothing, when consumer groups expressed concern such devices could be used to track movements of individual purchasers. The U.S. government is currently issuing RFID-enabled passports to track their own citizens, and is requiring other countries to issue their citizens RFID-enabled passports before they are allowed into the U.S. It is notable that though certain cryptographic security measures are applied in RFID chips held in passports, RFID technology could still be promoting instead of preventing identity theft. Canadian law enforcement has recently issued in-house warnings that criminals can be expected to attempt and succeed in hacking databases containing RFID data and abusing information thus gained to commit financial crimes .[xxii] By apprehending the potential of this technology in affecting consumer privacy Civil liberty organizations are trying to stop RFID tagging of consumer goods. Three of the most outspoken advocacy groups are: the Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), the American Civil Liberties Union (ACLU), and the Electronic Privacy Information Center (EPIC). The Privacy Guidelines of the Organization for Economic Co-operation and Development (OECD) offers useful advice related to the disclosure of RFID technology use and the purpose behind its use. The Privacy Guidelines of the Organisation for Economic Co-operation and Development (OECD) are placed below through Figure 06:

Openness, or Transparency.

RFID users must make public their policies and practices involving the use and maintenance of RFID systems, and there should be no secret databases. Individuals have a right to know when products or items in the retail environment contain RFID tags or readers. They also have the right to know the technical specifications of those devices. Labeling must be clearly displayed and easily understood. Any tag reading that occurs in the retail environment must be transparent to all parties. There should be no tag-reading in secret.



Purpose Specification.

RFID users must give notice of the purposes for which tags and readers are used.

- Collection limitation. The collection of information should be limited to that which is necessary for the purpose at hand.
- Accountability. RFID users are responsible for implementation of this technology and the associated data. RFID users should be legally responsible for complying with the principles. An accountability mechanism must be established. There must be entities in both industry and government to whom individuals can complain when these provisions have been violated.

Security Safeguards.

There must be security and integrity in transmission, databases, and system access. These should be verified by outside, third-party, publicly disclosed assessment.

- RFID Practices that Should be Flatly Prohibited: (a) Merchants must be prohibited from forcing or coercing customers into accepting live or dormant RFID tags in the products they buy.(b) There should be no prohibition on individuals to detect RFID tags and readers and disable tags on items in their possession.(c) RFID must not be used to track individuals absent informed and written consent of the data subject. Human tracking is inappropriate, either directly or indirectly, through clothing, consumer goods, or other items.(d) RFID should never be employed in a fashion to eliminate or reduce anonymity. For instance, RFID should not be incorporated into currency.

Many people are now starting to fear that literally everything on the planet could one day be tagged and this fear has led to the establishment of the Electronic Privacy Information Center (EPIC) and a coalition of privacy organisations to produce a position paper on the use of RFID in consumer products, recommending a framework of Fair Information Practices for data collected by the technology.[5] The coalition recommends following a set of minimum guidelines based in part on the eight-part Privacy Guidelines of the Organisation for Economic Co-operation and Development (OECD) while the larger assessment of RFID's societal implications takes place.[6] The position paper argues that RFID must undergo a formal technology assessment, that RFID tags should not be affixed to individual consumer products until such assessment takes place, and that under no circumstances should some uses of RFID be permitted, namely:

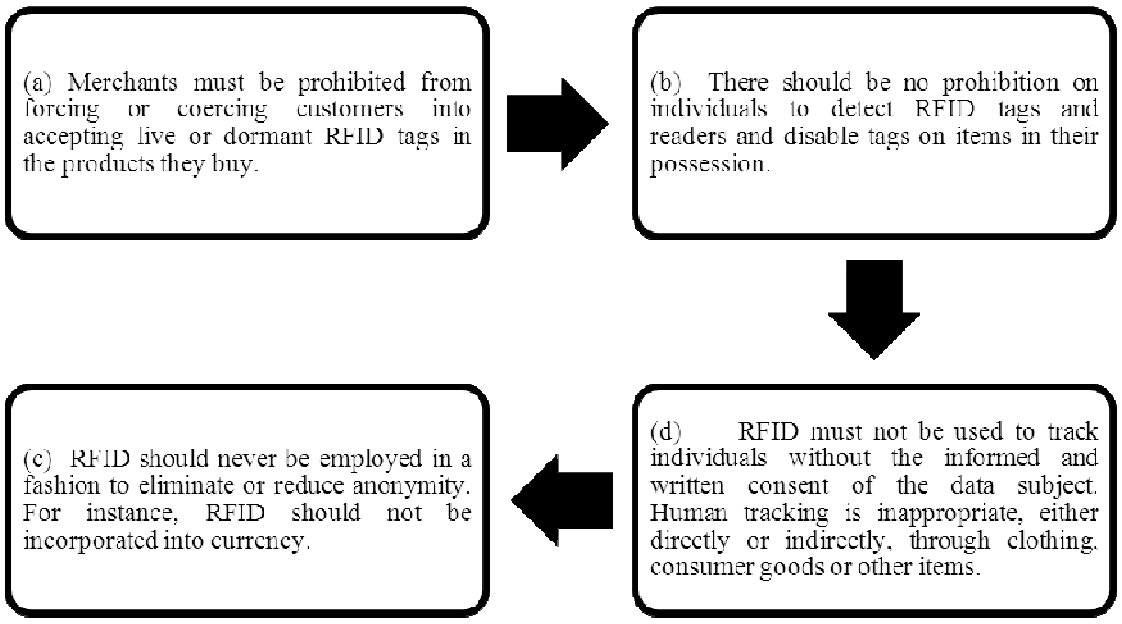


Figure 07: Electronic Privacy Information Center (EPIC) and the Coalition of Privacy Organisation's recommendations.

Approaches to Privacy: Legislative Measures in the Developed Countries

As RFID technology is not the stuff of science fiction novels, it is ready to be employed on a massive scale in today's world. But lac of regulatory mechanism makes it a risky technology which can be immensely used for intruding the privacy of others. Without regulation, RFID will be used to track both products and people. It is true that some laws in domestic level are quite equipped to deal the threat imposed by the RFID, but unified approach is so far absent in this field to regulate the misuse of RFID. For example, In the United States, several states have initiated RFID privacy legislation, most notably California, where State Senator Debra Bowen introduced similar legislation in 2004 to address consumer privacy issues. Her bill required businesses and agencies to notify consumers that an RFID system is in place that can track and collect information about them. The bill required consumers to give express consent before businesses or agencies could track and collect information about them via RFID. Additionally, the California bill required retailers obtain express consent before they are allowed to use loyalty cards in which they track purchases of the consumer. This consent is necessary because consumers are apprehensive about how the data collected by the RFID tags can be linked to an individual's credit card to identify them personally. The California bill required businesses to destroy or detach the RFID tags before consumers leave a store. However, the California legislature ultimately rejected Senator Bowen's bill. Fortunately, the state Utah passed a similar Bill, titled "Radio Frequency Identification- Right to Know Act," requires a retailer selling a product containing an RFID tag must inform the consumer about the tag's existence by labelling

the package or posting notices both near the product and also at the location where the consumer transaction will be completed. The notice must state that the product contains an RFID tag and that the tag can transmit information to a reader both before and after the sale. The signs must be conspicuous in size and location, unless the seller automatically disables the tag prior to the completion of the sale. Often overlooked in policy discussion is the REAL ID Act, recently passed by the U.S. legislature. This bill mandates the development of federal U.S. standards for drivers' licenses, and could stimulate wide deployment of RFID tags without preemptive measures. In Europe, any personal data collected and processed in relation to RFID would have to comply with EU data protection law in the form of the Data Protection Directive 1995. So any data would need to be processed fairly and lawfully, be used for specified, explicit and legitimate purposes, and not be kept for longer than is necessary. The person or organisation collecting and processing that data would also have to inform the individual of that fact and the purpose(s) of the data collection. Under the Directive, the data controller would, given the fears that anyone with a RFID reader will be able to read the tag information, need to make sure appropriate technical and organisational measures are in place to protect personal data against accidental or unlawful destruction or loss or disclosure. The European Commission is beginning to look at RFID as a separate issue. It has issued a consultation based on the conclusions it reached after an internal workshop on RFID tags in July 2003. It recommends action in three areas:

1. Ensuring worldwide interoperability of RFID tag systems and globally harmonised spectrum resources;
2. catalysing the initial demand for RFID systems; and
3. addressing the emerging concerns of privacy and user acceptance, including getting the RFID industry to formulate clear recommendations, codes of conduct and guidelines on the appropriate use of these technologies.

As said earlier, different legal regimes adopted different principles and approaches regarding this matter. Aptly, these regimes undertook a multi-layered strategy to ensure that RFID remains relevant, yet there should be certain pre-emptive actions available against intrusion of privacy. The Privacy Guidelines of the Organisation for Economic Co-operation and Development (OECD) are appeared to be sound, but its implementation to some extent remains uncertain as it is not obligatory to follow the guidelines.

Approaches to Privacy: Legislative Measures within Domestic Law

"There is a sacred realm of privacy for every man and woman where he makes his choices and decisions-a realm of his own essential rights and liberties into which the law, generally speaking, must not intrude."- Baron Geoffrey Fisher

Privacy is one of the most pressing issues associated with the deployment of information technology. A high degree of privacy is a marker of a civilized, open and democratic society. A society that protects privacy is a society that accords human rights a high priority. Privacy promotes liberty, democracy, pluralism, individual autonomy and social order. Informational privacy has an individual and societal value. Privacy is a fundamental human right. It reinforces human vanity and other ethical standards such as freedom of association and freedom of

expression. In recent days it has become one of the most essential human rights. Privacy is protected in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and in many other international and regional human rights treaties. Almost every country in the world promotes right of privacy and recognises the existence of this right within constitutional mechanisms. At a minimum level, these provisions include any basic right or freedom to which all human beings are entitled and in whose exercise a government may not interfere which comprises of rights of inviolability of the home and secrecy of communications and rights to access and control one's personal information. In many of the countries where privacy is not explicitly recognised in the constitution, the courts have found that right in other provisions. For example, the U. S. Constitution contains no express right to privacy but to a great extent there exist judicial precedents which confirm the existence of right of privacy. It is pertinent to note that Privacy issues are synonymous with any system of information collection and storage, and in the EU, the personal data to which the RFID data is being attached still has to be used in compliance with prevailing legislation. The Bangladesh Constitution recognises the right of privacy to home and correspondence. Article 43 states that: "Every citizen shall have the right, subject to any reasonable restrictions imposed by law in the interests of the security of the State, public order, public morality or public health (1) to be secured in his home against entry, search and seizure; and (2) to the privacy of his correspondence and other means of communication." It is unfortunate that in Bangladesh we do not have any law that explicitly deals with individuals' right of privacy. But there are provision placed in various laws that to some extent protects citizens' right of privacy. For example, in Section 509 of the Penal Code, it is mentioned that "Whoever, intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, shall be punished with simple imprisonment for a term which may extend to one year, or with fine, or with both."[xxiii] The scope and extent of Section 509 of the Penal Code is too narrow to cover the fundamental right of privacy. Further, Section 71 of The Telecommunications Act 2001 says that "a person commits an offence, if he intentionally listens to a telephone conversation between two other persons, and for such offence, he shall be liable to be sentenced to imprisonment for a term not exceeding 6 (six) months or to a fine not exceeding 50 (fifty) thousand taka or to both." Furthermore, it is mentioned in ICT Act 2006 , under sec 63(1) ,that "Save as otherwise provided by this Act or any other law for the time being in force, no person who, in pursuance of any of the powers conferred under this Act, or rules and regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material shall, without the consent of the person concerned, disclose such electronic record, book, register, correspondence, information, document or other material to any other person shall be regarded as an offence." 63(2) states that "whoever commits any offence under sub-section 63(1) of this section he shall be punishable with imprisonment for a term which may extend to two years, or with fine which may extend to taka two lakhs, or with both." Moreover, under sec 7 of the Right to Information Act, 2009 publication of certain types of information is not mandatory for upholding citizens specially consumers commercial privacy. In section 7(4) it is stated that "Information related to commercial or business confidence, copyright or intellectual property right, the disclosure of which would harm the intellectual property rights of any third party" is not mandatory for publishing under this Act. Further in section 7(8) is it specifically stated that "Information the disclosure of which would harm the

privacy of the personal life of an individual" shall not be disclosed to anyone under the Right to Information Act, 2009. As said before privacy issues in our domestic law were dealt very frivolously and lack of coordination between legal provisions are evident everywhere, despite the fact that privacy is a constitutional right and this right is protected by law. But deviation from this constitutional right enforced by Article 43 is evident in many occasions. The Telegraph Act 1885 allows interception of communications in the interest of public safety (s. 5) and prohibits unlawful interception (ss. 25, 26). The Telecommunications Act 2001 was amended by the Telecommunications (Amendment) Act 2006 to give police broad authority to intercept mobiles and demand information from providers. These laws to some extant be used against an intrusion of privacy caused by RFID. But proportionate response against data intrusion are absent in these provisions. All legal parameter that attempts to establish balance between intrusions of privacy and the right to privacy within our legal regime proved to be a little bit inconsistent with the concept of invasion of privacy through RFID technology. The legislative framework offered by the Telecommunications (Amendment) Act- 2006 and Information Communication Technology (ICT) Act-2006 somewhat failed to recognize and remedy invasion of privacy caused by technology such as RFID properly.

In this stage, the discussion demands the determination of legal status of RFID chips within Bangladeshi law. Under Telecommunications (Amendment) Act- 2006 RFID may fall within the ambit of "radio apparatus". Clause -25 of Telecommunications (Amendment) Act- 2006 defines "radio apparatus" as a device or combination of more than one device suitable for use in radio communication. Clause -26 of Telecommunications (Amendment) Act- 2006 further clarifies radio communication. It states that "radio communication or radio" means emission, transmission or reception of any sign, signal, picture, image, symbol or sound by means of radio wave of a frequency lower than 3000 Ghz and propagated in the space without any artificial guide. Most RFID produces uses frequency lower than 3000 Ghz, therefore falls within the ambit of Clause -25.[xxiv] A table is posted below which shows data transfer speed and RFID frequency bands used for modulating and demodulating a radio-frequency (RF) signal.

Band	Regulations	Range	Data speed	Remarks
120–150 kHz (LF)	Unregulated	10 cm	Low	Animal identification, factory data collection
13.56 MHz (HF)	ISM band worldwide	1 m	Low to moderate	Smart cards (MIFARE, ISO/IEC 14443)
433 MHz (UHF)	Short Range Devices	1–100 m	Moderate	Defence applications, with active tags
865-868 MHz (Europe) 902-928 MHz (North America) UHF	ISM band	1–2 m	Moderate to high	EAN, various standards
2450-5800 MHz (microwave)	ISM band	1–2 m	High	802.11 WLAN, Bluetooth standards

Source: Sen, Dipankar; Sen, Prosenjit; Das, Anand M. (2009), RFID For Energy and Utility Industries, PennWell, pp. 1-48

If a RFID product uses a frequency lower than 3000 Ghz and if a third-party unlawfully intercepts the radio communication between the RFID tag and reader, resulting unauthorised data access and intrusion of privacy then he may be liable for committing an offence under Section 67of Telecommunications (Amendment) Act- 2006. Under Section 67(1) of Telecommunications (Amendment) Act- 2006 it is stated that (1) No person shall- (a) without lawful excuse, create obstruction to or cause interference in radio communication or telecommunication; or (b) intercept any radio communication or telecommunication nor shall utilize or divulge the intercepted communication, unless the originator of the communication or the person to whom the originator intends to send it has consented to or approved the interception or divulgence. Further Section 67(2) of the Act says (2) A person commits an offence if he contravenes sub-section (1) and for such offence he shall be liable to be sentenced to imprisonment for a term not exceeding 3 (three) years or to a fine not exceeding 3 (three) lac taka or to both.

As said before RFID has revolutionised life in the 21st Century by fundamentally altering the relationship between consumer and retailer, citizen and State. Recent reports estimate that by 2012 almost 60 billion tags could be affixed to items worldwide, with 20 billion of the tags being affixed to consumer products and approximately half a million product-embedded RFID tags are used within Bangladesh. This gives birth to a more immediate concern relating to product-embedded active RFID tags. Potentially, every time the consumer is using, wearing or carrying the product and comes within range of an RFID terminal, information about that individual's location, buying preferences and consumption levels and periodicity will be collected and collated. Thus, the individual can be tracked and profiled. This personal database is extremely valuable for marketing purposes. The information can be mined by companies to facilitate unauthorised and unsolicited activities, such as the targeting of new direct marketing recipients, surveillance of consumer habits and predilections, deployment of dynamic pricing and differentiated treatment of consumers. The commercial dangers to privacy include identity theft, informational inequality where the collecting body is more powerful than the data subject, loss of the right to control information about oneself and the invisible nature of data collection. The consumer is ill prepared to protect their privacy. As there is no 'balanced law' relating to this subject matter in Bangladesh, the invasion of the physical and the informational privacy of the individual will undeniably affect the legal regime that deals with the concept of privacy. It is important to emphasise that RFID technology does not create new privacy problems. Rather, it greatly facilitates the opportunity for data collection, analysis and accumulation. As said before, the data collected by RFID tags is of great commercial benefit to companies and undertakings. The collation of personal data is not only of benefit to third party marketers: Organisations can control the supply chain from inception through to eventual disposal. This knowledge enables undertakings to track goods to an unprecedented extent and ensure that parallel importers are severely restricted in their ability to source non-authorised goods. Competition is distorted, restricted or even prevented in such a situation. For example, the interference with competitive forces threatens the internal market objective of the European Union. There are more than a few regulations are available in many countries regarding this sort of commercial espionage. But Bangladesh does not have sufficient regulatory mechanism to control commercial reconnaissance conducted through RFID. Fortunately Section67 (2) and 83 of the Telecommunications

(Amendment) Act- 2006 may be used for controlling commercial reconnaissance conducted through RFID. Section 83 of the Act deals with right to civil suits and other remedies for unlawful disclosure of message. Section 83 says that (1) If a person, on reasonable grounds, believes that a message sent or received by him has been or will be unlawfully disclosed, or that it has been or will be used in violation of the provisions of section 67(1) or 68(1)[xxv], he may, for prohibiting such disclosure or use or for realizing compensation from the person liable for such disclosure or use, file a civil suit in the court of Sub- Judge against the person so disclosing or using; and in such a suit the court may pass on order of injunction or award compensation or other relief as it considers appropriate. (2) If a person has been found guilty of an offence under section 67(1) or 68(1) and if, on the basis of the same occurrence, a civil suit is filed under sub-section (1), of this section, the certified copies of the evidence admitted in the criminal proceedings may be presented for admission in the civil suit to prove the alleged unlawful disclosure or use of a message; and the decision by which that person was found guilty shall, in relation to the relief prayed for, be deemed to be sufficient proof. (3) A civil suit under sub-section (1) shall be filed within 3 (three) years from the date on which the cause of action for the suit arose. (4) Filing of a civil suit by a person under this section shall not affect the exercise of his other rights including his right to seek other remedies. It is pertinent to note that Section 83 directly indicates massage and does not say anything about RFID contained information in 'electronic form'[xxvi]. We know massages are nothing but data[xxvii] and RFID also contains and transmits Data. Therefore massages or electronic record[xxviii] transmitted from a mobile to another mobile or interoperable device and a data interexchange through RFID carries same status. Thus, if data contained in RFID chip mishandled without any lawful excuse, civil suits and other remedies for unlawful disclosure of message can be invoked under Section 83 of Telecommunications (Amendment) Act- 2006. Further under Information Communication Technology (ICT) Act-2006 authorised users of RFID can have protection from Data theft and privacy intrusion. Section 54 of Information Communication Technology (ICT) Act-2006 states that "If any person, without permission of the owner or any person who is in charge of a computer, computer system or computer network,-- (a) accesses or secure access to such computer, computer system or computer networks for the purpose of destroying information or retrieving or collecting information or assists other to do so; (b) downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium…. then the above said activities shall be treated as offences of the said person ; (d) damages or causes to be damaged willingly in any computer, computer system or computer network, data, computer database or any other programmes residing in such computer, computer system or computer network; (2) If any person commits offence under sub-section (1) of this section, he shall be punishable with imprisonment for a term which may extend to ten years, or with fine which may extend to Taka ten lakhs, or with both." For applying Section 54 of the Act, it is first to be decided that whether computer, computer system or computer networks are equivalent to RFID Scanner and tag. It is true that RFID Scanners are not similar to a computer physically but it needs hardware and software to function. RFID Scanners and computers both require data inputs and complex matrix of programming. Both are not exact replica of each other due to their desired functions but both work same ways. On the other hand RFID tags are more than a pen drive with

Bluetooth quipped to transmit data or electronic records to paired RFID readers. It is pertinent to note that like computer network, RFID also maintains and channels information between tags and scanners using computer system. It also proses and preserves data with the help of computers and customised software. So in my opinion RFID contained electronic record or data may get protection under Section 54 of Information Communication Technology (ICT) Act-2006 as RFID systems are to some extent equivalent to any computer, computer system or computer network, computer database. Further under present Copy Right Law, data contained in RFID also enjoys protection from unauthorised usages.

RFID and Its Invasion Authorised by Public Authorities

When the public authorities become the intruders, the consequences are apt to prove more than a mere nuisance. For example, the UK allows the interception of telephone calls, emails, letters and faxes by authorisation of the Home Secretary rather than by a judge. In America there exists a similar system of warrantless surveillance operated by the National Security Agency. Bangladesh and the UK's system of interception without prior judicial authorisation or American system of warrantless surveillance is a threat to the privacy of an individual.[xxix] As said before, Section 97(Ka) Bangladesh Telecommunication Act-2001 empowers Minister or State Minister of Home Ministry to order the public authority to approve tapping of any telephone, or recording or intercepted message without prior authorisation of the judiciary. Further, section 97(Kha) of this Act states that any information obtained under section 97(Ka) shall be considered as an admissible evidence in all circumstances, even if it conflicts with Evidence Act 1872 or other statuary provisions. It means if surveillance evidence is obtained illegally or if a public authority acts beyond its jurisdiction in procuring surveillance evidence, that evidence should not be treated as inadmissible in the court. This is a pure inclusionary rule that undermines the individual's right of privacy. Moreover, the investigatory activities authorised by the Telecommunication Act 2001 inevitably makes an impact on the privacy of the affected individual. In most instances, it is clear that this impact constitutes an interference with the right to respect for private and family life, home and correspondence, as protected by our constitution[xxx]. I must admit that our law has failed to keep pace with the ever more sophisticated surveillance techniques like RFID and Section 97 may be used for legally accessing RFID data without the consent of the owners. The Telecommunication Act-2001 and its repeal fall far short of an effective Parliamentary response in regulating advanced technology such as RFID for conducting surveillance activities. It is unfortunate that our law still does not offer an effective regulatory system to deal with surveillance and interception conducted with the help of RFID. Thus the law remains weak in terms of the imposition of regulation and the protection for privacy in electronic communications.

Conclusion

Privacy, security and information control are an often neglected topic. RFID technology provides greatly expanded data collection capabilities and carries inherent technical vulnerabilities causing intrusion of privacy and data leakage. The permanence or quasi-permanence of RFID implants , attachable and non-detachable tags engenders significant human rights concerns in Bangladesh, which invades both the physical privacy and the informational privacy of the individual and threatens to undermine the discrete privacy spaces of the individual. Overtime, abrupt use of the RFID would collect a vast range of information about the individual's health, genetics, location, and levels of chemical, food and drink ingestion in Bangladesh. The information collected through RFID could be used to refuse insurance coverage or deny employment opportunities. In a futuristic ambient intelligent environment, it would be almost impossible for the individual to control who received, collected, processed and analysed this data in absence of proper regulatory provisions in Bangladesh. Robust underlying security architecture with well-established security management practices and controls along with proportionate legal framework are the key to the real-world implementation of higher level privacy-preserving RFID network.

References

Nathan Good, John Han, Elizabeth Miles, David Molnar, Deirdre Mulligan, Laura Quilter, Jennifer Urban, and David Wagner. Radio frequency identification and privacy with information goods. In Workshop on Privacy in the Electronic Society – WPES (To appear), Lecture Notes in Computer Science, Washington, DC, USA, October 2004. Springer-Verlag.

Challenge-response based RFID authentication protocol for distributed database environment. In Security in Pervasive Computing, number 3450 in Lecture Notes in Computer Science, pages 70–84, 2005.

Katherine Albrecht , Liz McIntyre, The Spychips Threat: Why Christians Should Resist RFID and Electronic Surveillance(1st Edition, Publisher: Thomas Nelson ,United Kingdom, 2006)

Larry Downes, The Laws of Disruption: Harnessing the New Forces that Govern Life and Business in the Digital Age (1st Edition, Publisher: Basic Books, California, 2009)

Daniel M. Dobkin The RF in RFID, Second Edition: UHF RFID in Practice (2nd Edition, Publisher: Newnes , 2012)

Klaus Finkenzeller (Author), Dörte Müller (Translator) RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication (3rd Edition, Publisher: Wiley, 2010)

F. Leslie Smith, John W. Wright and John W. Wrigth, Electronic Media and Government: The Regulation of Wireless and Wired Mass Communication in the United States (1st Edition, Publisher: Longman Publishing Group ,1994)

Paul Goldstein and Marketa Trimble , International Intellectual Property Law, Cases and Materials(3d Edition , Publisher: Foundation Press, 2012)

Deborah E. Bouchoux ,Intellectual Property: The Law of Trademarks, Copyrights, Patents, and Trade Secrets (4 edition ,Publisher: Delmar Cengage Learning; 2012)

Charles H. Kennedy , M. Veronica Pastor , An Introduction to International Telecommunications Law (1st edition, Publisher: Artech House , 1996)

Endnote

[i] Christian Floerkemeier and Frederic Thiesse (2005), EPC Technology. In D. Hutter and M. Ullmann, editors, Second International Conference on Security in Pervasive Computing (SPC 2005), number 3450 in Lecture Notes in Computer Science, pages 117–118. Springer-Verlag, Berlin Germany, 2005.

[ii] Simson Garfinkel (2002), RFID Bill of Rights. MIT Technology Review, page 35, October 2002.

[iii] Xingxin (Grace) Gao, Zhe (Alex) Xiang, Hao Wang, Jun Shen, Jian Huang, and Song Song(2004), An approach to security and privacy of RFID system for supply chain. In IEEE International Conference on E-Commerce Technology for Dynamic E-Business (CEC-East'04), pages 164–168. IEEE Computer Society, 2004.

[iv] GAO (2005), INFORMATON SECURITY: Radio Frequency Identification Technology in the Federal Government. Washington, DC: Government Accountability Office, May 2005. (www.gao.gov/new.items/d05551.pdf) retrieved :04/03/2013

[v] tag ID: I-Q32T w/LED

[vi] Roger Yu, Electronic Passports Set to Thwart Forgers, USA TODAY, Aug. 9, 2005, at 8B.

[vii] Gardiner Harris, Tiny Antennas to Keep Tabs on U.S. Drugs, N.Y. TIMES, Nov. 15,2004.

[viii] Mexican Officials Get Chipped, WIRED NEWS, Jul. 13, 2004 (noting that Mexico's Attorney General and several other government officials have had chips embedded under their skin to allow tracing in the event of a kidnapping, and to verify identity for accessing a computerized crime database).

[ix] Barcelona Clubbers Get Chipped, BBC NEWS, Sept. 29, 2005, available at http://news.bbc.co.uk/2/hi/technology/3697940.stm. retrieved :04/03/2013

[x] Verichip utilizes the implantable, passive RFID microchip, in their solutions for the purpose of automatic identification. About the size of a grain of rice, the microchip inserts just under the skin and contains only a unique, 16-digit identifier. In the future this chip may contain Global Positioning System (GPS) tracking capabilities. And unlike conventional forms of identification, the VeriChip cannot be lost, stolen, misplaced, or counterfeited. It is considered safe, secure, and will always be with you. Once inserted just under the skin, via a quick, outpatient procedure (much like getting a shot), the VeriChip can be scanned when necessary with a proprietary VeriChip reader, whether handheld or wall-mounted. A small amount of radio frequency energy passes from the reader energizing the dormant microchip which then emits a radio frequency signal transmitting the individuals unique verification number. This number can then be used for such purposes as accessing personal medical information in a password-protected database or assessing whether somebody has authority to enter into a high-security area. VeriChip has now been approved to offer an implantable FDA approved RFID microchip.

[xi] Jonathan Collins (2004), Tracking Medical Emergencies (Apr. 22, 2004), http://www.rfidjournal.com/article/articleview/901/1/1/ (on file with the North Carolina Journal of Law & Technology).

[xii] Kim Zetter (2005), School RFID Plan Gets an F, WIRED, Feb. 10, 2005, http://www.wired.com/news/privacy/0,1848,66554,00.html (on file with the North Carolina Journal of Law & Technology).

[xiii] http://www2.ministries-online.org/biometrics/rfidchip.html retrieved :04/03/2013

[xiv] JISC Technology and Standards Watch, May 2006 at p.9.

[xv] Privacy Rights Clearinghouse, RFID Position Statement of Consumer Privacy and Civil Liberties Organizations, Nov. 20, 2003, http://www.privacyrights.org/ar/RFIDposition.htm

[xvi] Privacy Rights Clearinghouse, RFID Position Statement of Consumer Privacy and Civil Liberties Organizations, Nov. 20, 2003, http://www.privacyrights.org/ar/RFIDposition.htm

[xvii] Germain, Jack M. (2005), RFID Technology Faced with Privacy Considerations. E-Commerce Times July 11, 2005.

[xviii] John Iwasaki(2006), You Can Lace 'Em Up, But You Can't Shut 'Em Up: Shoes Send Signals Into Air, For Anyone to Receive, SEATTLE POST-INTELLIGENCER, Dec. 1, 2006.

[xix] The Nike+iPod Sports Kit is a device which measures and records the distance and pace of a walk or run. The Nike+iPod consists of a small transmitter device attached to or embedded in a shoe, which communicates with either the Nike+ Sport band, a receiver plugged into an iPod Nano, or directly with a 2nd, 3rd, or 4th Generation iPod Touch, iPhone 3GS or iPhone 4 or a Nike+ Sport watch. If using the iPod or the iPhone 3GS, iTunes software can be used to view the walk or run history. On September 7, 2010, Nike released the Nike+ GPS App, which used a tracking engine powered by MotionX that does not require the separate shoe sensor. This application works using the accelerometer and GPS of the iPhone and the accelerometer of the iPod Touch (which does not currently contain a GPS chip). Source: http://en.wikipedia.org/wiki/Nike%2BiPod. Retrieved : 30th June 2012

[xx] Saponas and his fellow researchers posited several hypothetical scenarios, including how a (fictitious) obsessed ex-boyfriend could surreptitiously place the Nike transponder in the purse or other personal item of his ex-girlfriend and, with the help of a few strategically placed RFID readers, keep tabs on her whereabouts or stage "coincidental" meetings.

[xxi] Garfinkel, Simson L. (2004), The Trouble with RFID. The Nation, February 3, 2004.

[xxii] CISC (2007) ,The Use of Radio Frequency Identification Devices for Criminal Purposes. Sentinel Strategic Early Warning Assessment (4)2, June 2007.

[xxiii] https://www.privacyinternational.org/reports/state-of-legal-protections-in-asia/bangladesh Retrieved on 27/7/2012

[xxiv] Canadian law also considers RFID as radio apparatus. Source: RSS-Gen – General Requirements and Information for the Certification of Radio Apparatus http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf10202.html#s7

[xxv] Penalty for misuse of radio or telecommunication apparatus by employee.

[xxvi] "electronic form" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, microfilm, computer generated microfiche or similar device or technology…2(5) Information Communication Technology (ICT) Act-2006.

[xxvii] "data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed, or has been processed in a computer system or computer network, and may be in any form including computer printouts, magnetic or optical storage media, punch cards, punched tapes or stored internally in the memory of the computer…….2(10) Information Communication Technology (ICT) Act-2006.

[xxviii] "electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer generated microfiche…2(7) Information Communication Technology (ICT) Act-2006.

[xxix] American Civil Liberties Union v National Security Agency, US District Court, 18 August 2006 (Case no. 06-CV-10204).

[xxx] Article 48(b)